Tue, 19 Jun 2007, 10:41:04 AM EST

Search Query Display

Recent Search Queries

		Results
#1	((dpa <and> logic <and> selection)<in>metadata)	0
#2	((dpa <or> ~~differential power analysis~~)<in>metadata)	147
#3	((dpa <or> ~~differential power analysis~~)<in>metadata)	147

IEEE Xplore® RELEASE 2.3

Search Result - Print Format

< B

Key: IEEE JNL = IEEE Journal or Magazine, IEE JNL = IEE Journal or Magazine, IEEE CNF = IEEE Conference, IEE CNF = IEE Conference, IE STD = IEEE Standard

1. **Towards an in-situ endospore detection instrument**
Shafaat, H.S.; Cable, M.L.; Ikeda, M.K.; Kirby, J.P.; Pelletier, C.C.; Ponce, A.;
Aerospace, 2005 IEEE Conference
5-12 March 2005 Page(s):660 - 669
IEEE CNF

2. **Evaluation of Dynamic Voltage and Frequency Scaling as a Differential Power Analysis Countermeasure**
Baddam, K.; Zwolinski, M.;
VLSI Design, 2007. Held jointly with 6th International Conference on Embedded Systems., 20th International Conference on
Jan. 2007 Page(s):854 - 862
IEEE CNF

3. **Delay insensitive encoding and power analysis: a balancing act [cryptographic hardware protection]**
Kulikowski, K.J.; Ming Su; Smirnov, A.; Taubin, A.; Karpovsky, M.G.; MacDonald, D.;
Asynchronous Circuits and Systems, 2005. ASYNC 2005. Proceedings. 11th IEEE International Symposium on
14-16 March 2005 Page(s):116 - 125
IEEE CNF

4. **Network-assisted resource management for wireless data networks**
Qiu, X.; Chawla, K.; Chuang, J.C.-I.; Sollenberger, N.;
Selected Areas in Communications, IEEE Journal on
Volume 19, Issue 7, July 2001 Page(s):1222 - 1234
IEEE JNL

5. **Implementation aspects of the DPA-resistant logic style MDPL**
Popp, T.; Mangard, S.;
Circuits and Systems, 2006. ISCAS 2006. Proceedings. 2006 IEEE International Symposium on
21-24 May 2006 Page(s):4 pp.
IEEE CNF

6. **An Efficient Algorithm for DPA-resistent RSA**
Wang, Yi; Leiwo, Jussipekka; Srikanthan, Thambipillai; Jianwen, Luo;
Circuits and Systems, 2006. APCCAS 2006. IEEE Asia Pacific Conference on
4-7 Dec. 2006 Page(s):1659 - 1662
IEEE CNF

7. **AES-Based Security Coprocessor IC in 0.18-$muhbox m$CMOS With Resistance to Differential Power Analysis Side-Channel Attacks**
Hwang, D.D.; Tiri, K.; Hodjat, A.; Lai, B.-C.; Yang, S.; Schaumont, P.; Verbauwhede, I.;
Solid-State Circuits, IEEE Journal of
Volume 41, Issue 4, April 2006 Page(s):781 - 792
IEEE JNL

8. **Overcoming Glitches and Dissipation Timing Skews in Design of DPA-Resistant Cryptographic Hardware**
Lin, Kuan Jen; Fang, Shan Chien; Yang, Shih Hsien; Lo, Cheng Chia;
Design, Automation & Test in Europe Conference & Exhibition, 2007. DATE '07
April 2007 Page(s):1 - 6
IEEE CNF

9. **A Leak Resistant SoC to Counteract Side Channel Attacks**
Badrignans, B.; Mesquita, D.; Moraes, F.G.; Robert, M.; Sassatelli, G.; Torres, L.;
System-on-Chip, 2006. International Symposium on
Nov. 2006 Page(s):1 - 4
IEEE CNF

10. **Area and Power Efficient Synthesis of DPA-Resistant Cryptographic S-Boxes**
Giaconia, M.; Macchetti, M.; Regazzoni, F.; Schramm, K.;
VLSI Design, 2007. Held jointly with 6th International Conference on Embedded Systems., 20th International Conference on
Jan. 2007 Page(s):731 - 737
IEEE CNF

11. **A table masking countermeasure for low-energy secure embedded systems**
Gebotys, C.H.;
Very Large Scale Integration (VLSI) Systems, IEEE Transactions on
Volume 14, Issue 7, July 2006 Page(s):740 - 753
IEEE JNL

12. **DPA on quasi delay insensitive asynchronous circuits: formalization and improvement**
Bouesse, G.F.; Renaudin, M.; Dumont, S.; Germain, F.;
Design, Automation and Test in Europe, 2005. Proceedings
2005 Page(s):424 - 429 Vol. 1
IEEE CNF

13. **Efficient Solution for Misalignment of Signal in Side Channel Analysis**
Le, Thanh-Ha; Clediere, Jessy; Serviere, Christine; Lacoume, Jean-Louis;
Acoustics, Speech and Signal Processing, 2007. ICASSP 2007. IEEE International Conference on
Volume 2, 15-20 April 2007 Page(s):II-257 - II-260
IEEE CNF

14. **The Impact of the Implementation Style on Power Consumption and Security in Embedded Cryptosystems**
Muresan, R.; Yang, Z.;
Electrical and Computer Engineering, Canadian Conference on
May 2006 Page(s):1325 - 1328
IEEE CNF

15. **Improving DPA security by using globally-asynchronous locally-synchronous systems**
Gurkaynak, F.; Oetiker, S.; Kaeslin, H.; Felber, N.; Fichtner, W.;
Solid-State Circuits Conference, 2005. ESSCIRC 2005. Proceedings of the 31st European
12-16 Sept. 2005 Page(s):407 - 410
IEEE CNF

16. **A countermeasure against differential power analysis based on random delay insertion**
Bucci, M.; Luzzi, R.; Guglielmo, M.; Trifiletti, A.;
Circuits and Systems, 2005. ISCAS 2005. IEEE International Symposium on
23-26 May 2005 Page(s):3547 - 3550 Vol. 4
IEEE CNF

17. **Towards an AES crypto-chip resistant to differential power analysis**
Pramstaller, N.; Gurkaynak, F.K.; Haene, S.; Kaeslin, H.; Felber, N.; Fichtner, W.;
Solid-State Circuits Conference, 2004. ESSCIRC 2004. Proceeding of the 30th European
21-23 Sept. 2004 Page(s):307 - 310
IEEE CNF

18. **SIMS depth profiling and SRIM simulation to lower energy antimony implantation into silicon**
Yupu Li; Shyue, J.; Hunter, J.; McComb, B.; Chun, M.; Doherty, R.; Foad, M.;
Ion Implantation Technology. 2002. Proceedings of the 14th International Conference on

22-27 Sept. 2002 Page(s):625 - 628

IEEE CNF

19. **Transmission of optical communication signals by distributed parametric amplification**
Kalogerakis, G.; Marhic, M.E.; Wong, K.K.-Y.; Kazovsky, L.G.;
Lightwave Technology, Journal of
Volume 23, Issue 10, Oct. 2005 Page(s):2945 - 2953

IEEE JNL

20. **Secure contactless smartcard ASIC with DPA protection**
Rakers, P.; Connell, L.; Collins, T.; Russell, D.;
Solid-State Circuits, IEEE Journal of
Volume 36, Issue 3, March 2001 Page(s):559 - 565

IEEE JNL

21. **An on-chip signal suppression countermeasure to power analysis attacks**
Ratanpal, G.B.; Williams, R.D.; Blalock, T.N.;
Dependable and Secure Computing, IEEE Transactions on
Volume 1, Issue 3, July-Sep 2004 Page(s):179 - 189

IEEE JNL

22. **An all-digital PLL with cascaded dynamic phase average loop for wide multiplication range applications**
Pao-Lung Chen; Ching-Che Chung; Chen-Yi Lee;
Circuits and Systems, 2005. ISCAS 2005. IEEE International Symposium on
23-26 May 2005 Page(s):4875 - 4878 Vol. 5

IEEE CNF

23. **A side-channel leakage free coprocessor IC in 0.18/spl mu/m CMOS for embedded AES-based cryptographic and biometric processing**
Tiri, K.; Hwang, D.; Hodjat, A.; Lai, B.; Yang, S.; Schaumont, P.; Verbauwhede, I.;
Design Automation Conference, 2005. Proceedings. 42nd
13-17 June 2005 Page(s):222 - 227

IEEE CNF

24. **Comparative study of uplink and downlink beamforming algorithms in UTRA/TDD**
Pelletier, B.; Jian Mao; Champagne, B.;
Vehicular Technology Conference, 2004. VTC 2004-Spring. 2004 IEEE 59th
Volume 2, 17-19 May 2004 Page(s):1162 - 1166 Vol.2

IEEE CNF

25. **Energy-aware design techniques for differential power analysis protection**
Benini, L.; Omerbegovic, E.; Macii, A.; Poncino, M.; Macii, E.; Pro, F.;
Design Automation Conference, 2003. Proceedings
2-6 June 2003 Page(s):36 - 41

IEEE CNF

Terms used **dpa differential power analysis** Found **98** of **204,472**

Sort results by: relevance
Display results: expanded form
Save results to a Binder
Search Tips
Open results in a new window
Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 20 of 98 Result page: **1** 2 3 4 5 next

Relevance scale

1 Digital circuits design: Current mask generation: a transistor level security against DPA attacks
Daniel Mesquita, Jean-Denis Techer, Lionel Torres, Gilles Sassatelli, Gaston Cambon, Michel Robert, Fernando Moraes
September 2005 **Proceedings of the 18th annual symposium on Integrated circuits and system design SBCCI '05**
Publisher: ACM Press
Full text available: pdf(513.86 KB) Additional Information: full citation, abstract, references, index terms

The physical implementation of cryptographic algorithms may leak to some attacker security information by the side channel data, as power consumption, timing, temperature or electromagnetic emanation. The Differential Power Analysis (DPA) is a powerful side channel attack, based only on the power consumption information. There are some countermeasures proposed at algorithmic or architectural level that are expensive and/or complexes. This paper addresses the DPA attack problem by a novel and eff ...

Keywords: DPA, countermeasures, cryptography, side channel attacks

2 DPA on Quasi Delay Insensitive Asynchronous Circuits: Formalization and Improvement
G. F. Bouesse, M. Renaudin, S. Dumont, Fabien Germain
March 2005 **Proceedings of the conference on Design, Automation and Test in Europe - Volume 1 DATE '05**
Publisher: IEEE Computer Society
Full text available: pdf(515.19 KB) Additional Information: full citation, abstract, index terms

The purpose of this paper is to formally specify a flow devoted to the design of Differential Power Analysis (DPA) resistant QDI asynchronous circuits. The paper first proposes a formal modeling of the electrical signature of QDI asynchronous circuits. The DPA is then applied to the formal model in order to identify the source of leakage of this type of circuits. Finally, a complete design flow is specified to minimize the information leakage. The relevancy and efficiency of the approach is demo ...

3 Crypto blocks and security: Overcoming glitches and dissipation timing skews in design of DPA-resistant cryptographic hardware
Kuan Jen Lin, Shan Chien Fan, Shih Hsien Yang, Cheng Chia Lo
April 2007 **Proceedings of the conference on Design, automation and test in Europe**

DATE '07
Publisher: ACM Press
Full text available: pdf(304.21 KB) Additional Information: full citation, abstract, references

Cryptographic embedded systems are vulnerable to Differential Power Analysis (DPA) attacks. In this paper, we propose a logic design style, called as Precharge Masked Reed-Muller Logic (PMRML) to overcome the glitch and Dissipation Timing Skew (DTS) problems in design of DPA-resistant cryptographic hardware. Both problems can significantly reduce the DPA-resistance. To our knowledge, the DTS problem and its countermeasure have not been reported. The PMRML design can be fully realized using co ...

4 Design of secure cryptography against the threat of power-attacks in DSP-embedded processors
Catherine H. Gebotys
February 2004 **ACM Transactions on Embedded Computing Systems (TECS)**, Volume 3 Issue 1
Publisher: ACM Press
Full text available: pdf(214.56 KB) Additional Information: full citation, abstract, references, citings, index terms

Embedded wireless devices require secure high-performance cryptography in addition to low-cost and low-energy dissipation. This paper presents for the first time a design methodology for security on a VLIW complex DSP-embedded processor core. Elliptic curve cryptography is used to demonstrate the design for security methodology. Results are verified with real dynamic power measurements and show that compared to previous research a 79% improvement in performance is achieved. Modification o ...

Keywords: VLIW

5 Architectures for cryptography and security applications: Simulation models for side-channel information leaks
Kris Tiri, Ingrid Verbauwhede
June 2005 **Proceedings of the 42nd annual conference on Design automation DAC '05**
Publisher: ACM Press
Full text available: pdf(244.28 KB) Additional Information: full citation, abstract, references, index terms

Small, embedded integrated circuits (ICs) such as smart cards are vulnerable to so-called side-channel attacks (SCAs). The attacker can gain information by monitoring the power consumption, execution time, electromagnetic radiation and other information that is leaked by the switching behavior of digital CMOS gates. Ever since power attacks have been introduced in 1999, many countermeasures have been proposed. Often a significant increase in security has been touted. We will show that in order t ...

Keywords: countermeasure, differential power analysis, encryption, security IC, side-channel attack, simulation model, smart card

6 A Logic Level Design Methodology for a Secure DPA Resistant ASIC or FPGA Implementation
Kris Tiri, Ingrid Verbauwhede
February 2004 **Proceedings of the conference on Design, automation and test in Europe - Volume 1 DATE '04**
Publisher: IEEE Computer Society
Full text available: pdf(143.96 KB) Additional Information: full citation, abstract, citings, index terms

This paper describes a novel design methodology to implement a secure DPA resistant

crypto processor. The methodology is suitable for integration in a common automated standard cell ASIC or FPGA design flow. The technique combines standard building blocks to make new'compound standard cells, which have a close to constant power consumption. Experimental results indicate a 50 times reduction in the power consumption fluctuations.

7 A split-mask countermeasure for low-energy secure embedded systems

Catherine H. Gebotys

August 2006 **ACM Transactions on Embedded Computing Systems (TECS)**, Volume 5 Issue 3

Publisher: ACM Press

Full text available: pdf(1.62 MB) Additional Information: full citation, abstract, references, index terms

Future wireless embedded devices will be increasingly powerful, supporting many more applications, including one of the most crucial---security. Although many embedded devices offer more resistance to bus---probing attacks because of their compact size, susceptibility to power or electromagnetic analysis attacks must be analyzed. This paper presents a new split-mask countermeasure to thwart low-order differential power analysis (DPA) and differential EM analysis (DEMA). For the first time, real- ...

Keywords: EM analysis, Side channel analysis, countermeasures, power attacks

8 Architectures for cryptography and security applications: A side-channel leakage free coprocessor IC in 0.18µm CMOS for embedded AES-based cryptographic and biometric processing

K. Tiri, D. Hwang, A. Hodjat, B. Lai, S. Yang, P. Schaumont, I. Verbauwhede

June 2005 **Proceedings of the 42nd annual conference on Design automation DAC '05**

Publisher: ACM Press

Full text available: pdf(2.92 MB) Additional Information: full citation, abstract, references, citings, index terms

Security ICs are vulnerable to side-channel attacks (SCAs) that find the secret key by monitoring the power consumption and other information that is leaked by the switching behavior of digital CMOS gates. This paper describes a side-channel attack resistant coprocessor IC and its design techniques. The IC has been fabricated in 0.18µm CMOS. The coprocessor, which is used for embedded cryptographic and biometric processing, consists of four components: an Advanced Encryption Standard (AES) ...

Keywords: countermeasure, differential power analysis, encryption, security IC, side-channel attack, smart card

9 Work-in-progress session on innovative topics: Security wrappers and power analysis for SoC technologies

C. H. Gebotys, Y. Zhang

October 2003 **Proceedings of the 1st IEEE/ACM/IFIP international conference on Hardware/software codesign and system synthesis CODES+ISSS '03**

Publisher: ACM Press

Full text available: pdf(790.57 KB) Additional Information: full citation, abstract, references, citings, index terms

Future wireless internet enabled devices will be increasingly powerful supporting many more applications including one of the most crucial, security. Although SoCs offer more resistance to bus probing attacks, power/EM attacks on cores and network snooping attacks by malicious code are relevant. This paper presents a methodology for security on NoC at both the network level (or transport layer) and at the core level (or application

layer) is proposed. For the first time a low cost security wrapp ...

Keywords: VLIW, adiabatic, design, performance, security

10 Poster: A secure fingerprint matching technique

Shenglin Yang, Ingrid M. Verbauwhede

November 2003 **Proceedings of the 2003 ACM SIGMM workshop on Biometrics methods and applications WBMA '03**

Publisher: ACM Press

Full text available: pdf(452.10 KB) Additional Information: full citation, abstract, references, citings, index terms

In this paper, we propose a novel robust secure fingerprint matching technique, which is secure against side channel attacks. An algorithm based on the local structure of the minutiae is presented to match the fingerprints. The main contribution is the careful division of the fingerprint recognition system into two parts: a secure part and a non-secure part. Only the relative small secure part, which contains sensitive biometric template information, requires realization in specialized DPA-proof ...

Keywords: DPA-proof, embedded system, fingerprint recognition, secure matching

11 Reliability and security: Java cryptography on KVM and its performance and security optimization using HW/SW co-design techniques

Yusuke Matsuoka, Patrick Schaumont, Kris Tiri, Ingrid Verbauwhede

September 2004 **Proceedings of the 2004 international conference on Compilers, architecture, and synthesis for embedded systems CASES '04**

Publisher: ACM Press

Full text available: pdf(188.08 KB) Additional Information: full citation, abstract, references, citings, index terms

This paper describes a design approach to include and optimize Java based cryptographic applications into resource limited embedded devices.For easy prototyping and to be platform independent, the security applications are first developed in Java. Two Java cryptographic libraries, the Bouncy Castle API and the IAIK API are ported to a real embedded device for cost and performance evaluation. It requires 0.88Mbytes to 1.2Mbytes in the KVM footprint size and a few milliseconds to run secret key al ...

Keywords: cryptography, design, embedded systems, java, security

12 A VLSI Design Flow for Secure Side-Channel Attack Resistant ICs

Kris Tiri, Ingrid Verbauwhede

March 2005 **Proceedings of the conference on Design, Automation and Test in Europe - Volume 3 DATE '05**

Publisher: IEEE Computer Society

Full text available: pdf(289.79 KB) Additional Information: full citation, abstract, index terms

This paper presents a digital VLSI design flow to create secure, side-channel attack (SCA) resistant integrated circuits. The design flow starts from a normal design in a hardware description language such as VHDL or Verilog and provides a direct path to a SCA resistant layout. Instead of a full custom layout or an iterative design process with extensive simulations, a few key modifications are incorporated in a regular synchronous CMOS standard cell design flow. We discuss the basis for side-ch ...

13 Power Attack Resistant Cryptosystem Design: A Dynamic Voltage and Frequency

Switching Approach
Shengqi Yang, Wayne Wolf, N. Vijaykrishnan, D. N. Serpanos, Yuan Xie
March 2005 **Proceedings of the conference on Design, Automation and Test in Europe - Volume 3 DATE '05**
Publisher: IEEE Computer Society
Full text available: pdf(291.83 KB) Additional Information: full citation, abstract, index terms

A novel power attack resistant cryptosystem is presented in this paper. Security in digital computing and communication is becoming increasingly important. Design techniques that can protect cryptosystems from leaking information have been studied by several groups. Power attacks, which infer program behavior from observing power supply current into a processor core, are important forms of attacks. Various methods have been proposed to countermeasure the popular and efficient power attacks. Howe ...

14 Masking the Energy Behavior of DES Encryption
H. Saputra, N. Vijaykrishnan, M. Kandemir, M. J. Irwin, R. Brooks, S. Kim, W. Zhang
March 2003 **Proceedings of the conference on Design, Automation and Test in Europe - Volume 1 DATE '03**
Publisher: IEEE Computer Society
Full text available: pdf(264.41 KB) Publisher Site Additional Information: full citation, abstract, citings, index terms

Smart cards are vulnerable to both invasive and non-invasive attacks. Specifically, non-invasive attacks using power and timing measurements to extract the cryptographic key has drawn a lot of negative publicity for smart card usage. The power measurement techniques rely on the data-dependent energy behavior of the underlying system. Further, power analysis can be used to identify the specific portions of the program being executed to induce timing glitches that may in turn help to bypass key ch ...

15 New techniques for security and reliability enhancement in embedded systems: Current flattening in software and hardware for security applications
Radu Muresan, Catherine Gebotys
September 2004 **Proceedings of the 2nd IEEE/ACM/IFIP international conference on Hardware/software codesign and system synthesis CODES+ISSS '04**
Publisher: ACM Press
Full text available: pdf(344.68 KB) Additional Information: full citation, abstract, references, index terms

This paper presents a new current flattening technique applicable in software and hardware. This technique is important in embedded cryptosystems since power analysis attacks (that make use of the current variation dependency on data and program) compromise the security of the system. The technique flattens the current internally by exploiting current consumption differences at the instruction level. Code transformations supporting current variation reductions due to program dependencies are pre ...

Keywords: current flattening, hardware architecture, power analysis attacks

16 Uniformly-Switching Logic for Cryptographic Hardware
Igor L. Markov, Dmitri Maslov
March 2005 **Proceedings of the conference on Design, Automation and Test in Europe - Volume 1 DATE '05**
Publisher: IEEE Computer Society
Full text available: pdf(118.50 KB) Additional Information: full citation, abstract, index terms

Recent work on Differential Power Analysis shows that even mathematically-secure cryptographic protocols may be vulnerable at the physical implementation level. By measuring energy consumed by a working digital circuit, one can glean enough

information to break encryption. Thwarting such attacks requires a new approach to logic and physical design. In this work, we seek to equalize switching activity of a circuit over all possible inputs and input transitions by adding redundant gates and increa ...

17 High Security Smartcards

M. Renaudin, F. Bouesse, Ph. Proust, J. P. Tual, L. Sourgen, F. Germain

February 2004 **Proceedings of the conference on Design, automation and test in Europe - Volume 1 DATE '04**

Publisher: IEEE Computer Society

Full text available: pdf(86.43 KB) Additional Information: full citation, abstract, citings, index terms

New consumer appliances such as PDA, Set Top Box, GSM/UMTS terminals enable an easy access to the internet and strongly contribute to the development of e-commerce and m-commerce services. Tens of billion payments are made using cards today, and this is expected to grow in a near future. Smartcard platforms will enable operators and service providers to design and deploy new e- and m-commerce services. This development can onlybe achieved if a high level of security is guaranteed for the transac ...

18 Security as a new dimension in embedded system design: Security as a new dimension in embedded system design

Srivaths Ravi, Paul Kocher, Ruby Lee, Gary McGraw, Anand Raghunathan

June 2004 **Proceedings of the 41st annual conference on Design automation DAC '04**

Publisher: ACM Press

Full text available: pdf(209.10 KB) Additional Information: full citation, abstract, references, citings, index terms

The growing number of instances of breaches in information security in the last few years has created a compelling case for efforts towards secure electronic systems. Embedded systems, which will be ubiquitously used to capture, store, manipulate, and access data of a sensitive nature, pose several unique and interesting security challenges. Security has been the subject of intensive research in the areas of cryptography, computing, and networking. However, despite these efforts, *security is ...*

***Keywords**: PDAs, architectures, battery life, cryptography, design, design methodologies, digital rights management, embedded systems, performance, security, security processing, security protocols, sensors, software attacks, tamper resistance, trusted computing, viruses*

19 Security in embedded systems: Design challenges

Srivaths Ravi, Anand Raghunathan, Paul Kocher, Sunil Hattangady

August 2004 **ACM Transactions on Embedded Computing Systems (TECS)**, Volume 3 Issue 3

Publisher: ACM Press

Full text available: pdf(3.67 MB) Additional Information: full citation, abstract, references, citings, index terms, review

Many modern electronic systems---including personal computers, PDAs, cell phones, network routers, smart cards, and networked sensors to name a few---need to access, store, manipulate, or communicate sensitive information, making security a serious concern in their design. Embedded systems, which account for a wide range of products from the electronics, semiconductor, telecommunications, and networking industries, face some of the most demanding security concerns---on the one hand, they are oft ...

Keywords: Embedded systems, architecture, authentication, battery life, cryptographic algorithms, decryption, encryption, hardware design, processing requirements, security, security attacks, security protocols, tamper resistance

20 Device, interconnect, and power optimization for nano-CMOS: Analysis of data dependence of leakage current in CMOS cryptographic hardware

Jacopo Giorgetti, Giuseppe Scotti, Andrea Simonetti, Alessandro Trifiletti

March 2007 **Proceedings of the 17th great lakes symposium on Great lakes symposium on VLSI GLSVLSI '07**

Publisher: ACM Press

Full text available: pdf(1.01 MB) Additional Information: full citation, abstract, references, index terms

A novel power analysis technique for CMOS cryptographic hardware based on leakage power consumption measurements is presented. Algorithms and models to predict the input vector for maximum and minimum leakage currentallin CMOS gates are reviewed. Extensive transistor level simulations on a simple CMOS crypto core are presented. Leakage current measurements carried out on an ASIC for cryptographic applications implemented in a 0.13 um CMOS technology are reported. The results of this work show th ...

Keywords: cryptographic hardware, leakage power consumption, side channel analysis

Results 1 - 20 of 98 Result page: **1** 2 3 4 5 next

Terms used **dpa differential power analysis redundant**

Found **91** of **204,472**

Sort results by relevance

Display results expanded form

Save results to a Binder

Search Tips

Open results in a new window

Try an Advanced Search

Try this search in The ACM Guide

Results 1 - 20 of 91

Result page: **1** 2 3 4 5 next

Relevance scale

1 Design of secure cryptography against the threat of power-attacks in DSP-embedded processors

Catherine H. Gebotys

February 2004 **ACM Transactions on Embedded Computing Systems (TECS)**, Volume 3 Issue 1

Publisher: ACM Press

Full text available:

Full text available: pdf(244.28 KB) Additional Information: full citation, abstract, references, index terms

Small, embedded integrated circuits (ICs) such as smart cards are vulnerable to so-called side-channel attacks (SCAs). The attacker can gain information by monitoring the power consumption, execution time, electromagnetic radiation and other information that is leaked by the switching behavior of digital CMOS gates. Ever since power attacks have been introduced in 1999, many countermeasures have been proposed. Often a significant increase in security has been touted. We will show that in order t ...

Keywords: countermeasure, differential power analysis, encryption, security IC, side-channel attack, simulation model, smart card

4 Design analysis techniques: Energy-aware design techniques for differential power analysis protection

Luca Benini, Alberto Macii, Enrico Macii, Elvira Omerbegovic, Fabrizio Pro, Massimo Poncino
June 2003 **Proceedings of the 40th conference on Design automation DAC '03**
Publisher: ACM Press

Full text available: pdf(286.41 KB) Additional Information: full citation, abstract, references, citings, index terms

Differential power analysis is a very effective cryptanalysis technique that extracts information on secret keys by monitoring instantaneous power consumption of cryptoprocessors. To protect against differential power analysis, power supply noise is added in cryptographic computations, at the price of an increase in power consumption. We present a novel technique, based on well-known power-reducing transformations coupled with randomized clock gating, that introduces a significant amount of scra ...

Keywords: differential power analysis, low-power design

5 A Logic Level Design Methodology for a Secure DPA Resistant ASIC or FPGA Implementation

Kris Tiri, Ingrid Verbauwhede
February 2004 **Proceedings of the conference on Design, automation and test in Europe - Volume 1 DATE '04**
Publisher: IEEE Computer Society
Full text available: pdf(143.96 KB) Additional Information: full citation, abstract, citings, index terms

This paper describes a novel design methodology to implement a secure DPA resistant crypto processor. The methodology is suitable for integration in a common automated standard cell ASIC or FPGA design flow. The technique combines standard building blocks to make new'compound standard cells, which have a close to constant power consumption. Experimental results indicate a 50 times reduction in the power consumption fluctuations.

6 A VLSI Design Flow for Secure Side-Channel Attack Resistant ICs

Kris Tiri, Ingrid Verbauwhede
March 2005 **Proceedings of the conference on Design, Automation and Test in Europe - Volume 3 DATE '05**
Publisher: IEEE Computer Society
Full text available: pdf(289.79 KB) Additional Information: full citation, abstract, index terms

This paper presents a digital VLSI design flow to create secure, side-channel attack (SCA) resistant integrated circuits. The design flow starts from a normal design in a hardware description language such as VHDL or Verilog and provides a direct path to a SCA resistant layout. Instead of a full custom layout or an iterative design process with extensive

simulations, a few key modifications are incorporated in a regular synchronous CMOS standard cell design flow. We discuss the basis for side-ch ...

7 High Security Smartcards
M. Renaudin, F. Bouesse, Ph. Proust, J. P. Tual, L. Sourgen, F. Germain
February 2004 **Proceedings of the conference on Design, automation and test in Europe - Volume 1 DATE '04**
Publisher: IEEE Computer Society
Full text available: pdf(86.43 KB) Additional Information: full citation, abstract, citings, index terms

New consumer appliances such as PDA, Set Top Box, GSM/UMTS terminals enable an easy access to the internet and strongly contribute to the development of e-commerce and m-commerce services. Tens of billion payments are made using cards today, and this is expected to grow in a near future. Smartcard platforms will enable operators and service providers to design and deploy new e- and m-commerce services. This development can onlybe achieved if a high level of security is guaranteed for the transac ...

8 Security as a new dimension in embedded system design: Security as a new dimension in embedded system design
Srivaths Ravi, Paul Kocher, Ruby Lee, Gary McGraw, Anand Raghunathan
June 2004 **Proceedings of the 41st annual conference on Design automation DAC '04**
Publisher: ACM Press
Full text available: pdf(209.10 KB) Additional Information: full citation, abstract, references, citings, index terms

The growing number of instances of breaches in information security in the last few years has created a compelling case for efforts towards secure electronic systems. Embedded systems, which will be ubiquitously used to capture, store, manipulate, and access data of a sensitive nature, pose several unique and interesting security challenges. Security has been the subject of intensive research in the areas of cryptography, computing, and networking. However, despite these efforts, *security is ...*

***Keywords**: PDAs, architectures, battery life, cryptography, design, design methodologies, digital rights management, embedded systems, performance, security, security processing, security protocols, sensors, software attacks, tamper resistance, trusted computing, viruses*

9 Practical experiences: Security-driven exploration of cryptography in DSP cores
Catherine H. Gebotys
October 2002 **Proceedings of the 15th international symposium on System Synthesis ISSS '02**
Publisher: ACM Press
Full text available: pdf(1.04 MB) Additional Information: full citation, abstract, references, index terms

With the popularity of wireless communication devices a new important dimension of embedded systems design has arisen, that of security. This paper presents for the first time design exploration for secure implementation of cryptographic applications on a complex DSP processor core. A new metric for security, the implementation security index, is introduced for measuring resistance to power attacks. Elliptic curve cryptographic algorithms are used to demonstrate and quantize security, energy, pe ...

Keywords: DSP, low energy, methodology, power analysis attack

10 Security on FPGAs: State-of-the-art implementations and attacks
Thomas Wollinger, Jorge Guajardo, Christof Paar

August 2004 **ACM Transactions on Embedded Computing Systems (TECS)**, Volume 3 Issue 3
Publisher: ACM Press
Full text available: pdf(296.79 KB) Additional Information: full citation, abstract, references, index terms

In the last decade, it has become apparent that embedded systems are integral parts of our every day lives. The wireless nature of many embedded applications as well as their omnipresence has made the need for security and privacy preserving mechanisms particularly important. Thus, as field programmable gate arrays (FPGAs) become integral parts of embedded systems, it is imperative to consider their security as a whole. This contribution provides a state-of-the-art description of security issues ...

Keywords: Cryptography, FPGA, attacks, cryptographic applications, reconfigurable hardware, reverse engineering, security

11 Power modeling and optimization for embedded systems: Energy-efficient data scrambling on memory-processor interfaces
Luca Benini, Angelo Galati, Alberto Macii, Enrico Macii, Massimo Poncino
August 2003 **Proceedings of the 2003 international symposium on Low power electronics and design ISLPED '03**
Publisher: ACM Press
Full text available: pdf(147.39 KB) Additional Information: full citation, abstract, references, index terms

Crypto-processors are prone to security attacks based on the observation of their power consumption profile. We propose new techniques for increasing the non-determinism of such profile, which rely on the idea of introducing randomness in the bus data transfers. This is achieved by combining data scrambling with energy-efficient bus encoding, thus providing high information protection at no energy cost.Results on a set of bus traces originated by real-life applications demonstrate the applicabil ...

Keywords: bus encoding, data scrambling, power attacks

12 URPR—An extension of URCR for software pipelining
B. Su, S. Ding, J. Xia
December 1986 **ACM SIGMICRO Newsletter , Proceedings of the 19th annual workshop on Microprogramming MICRO 19**, Volume 17 Issue 4
Publisher: ACM Press
Full text available: pdf(762.16 KB) Additional Information: full citation, abstract, references, citings, index terms

The software pipeline technique is an effective approach to optimizing loops in array processor programs, but existing methods are of high complexity and the results may not be satisfactory. This paper introduces the URPR algorithm, an extension of the microcode loop compaction algorithm URCR. Firstly, unroll the loop(the number of unrolled loop bodies relies on the inter-body data dependency); secondly, pipeline the unrolled loop bodies one by one; and finally, a new optimized l ...

13 Draft Proposed: American National Standard—Graphical Kernel System
Technical Committee X3H3 - Computer Graphics
February 1984 **ACM SIGGRAPH Computer Graphics**, Volume 18 Issue SI
Publisher: ACM Press
Full text available: pdf(16.07 MB) Additional Information: full citation

14 VLSI design: A novel architecture for power maskable arithmetic units

L. Benini, A. Macii, E. Macii, E. Omerbegovic, M. Poncino, F. Pro

April 2003 **Proceedings of the 13th ACM Great Lakes symposium on VLSI GLSVLSI '03**

Publisher: ACM Press

Full text available: pdf(166.52 KB) Additional Information: full citation, abstract, references, citings, index terms

Power maskable units have been proposed as a viable solution for preventing side-channel attacks to cryptoprocessors. This paper presents a novel architecture for the implementation of a class of such kinds of units, namely arithmetic components, which find wide usage in cryptographic applications and which are not suitable to traditional masking techniques. Results of extensive exploration and architectural trade-off analysis show the viability of the proposed solution.

Keywords: cryptography, low-power design, security

15 Linking the behavioral and structural dominis of representation in a synthesis system

Robert L. Blackburn, Donald E. Thomas

June 1985 **Proceedings of the 22nd ACM/IEEE conference on Design automation DAC '85**

Publisher: ACM Press

Full text available: pdf(865.37 KB) Additional Information: full citation, abstract, references, citings, index terms

Hierarchical design representation can be a useful approach to the problem of handling the complexity of digital designs. A means of linking together hierarchical behavioral representations in a design system is presented. Along with other information, this linking correlates the abstract behavior and logical structure together, opening the way for multilevel analysis aids that include these levels. Multilevel simulation is briefly discussed.

16 Digital RF processor (DRP/spl trade/) for cellular phones

R. B. Staszewski, K. Muhammad, D. Leipold

May 2005 **Proceedings of the 2005 IEEE/ACM International conference on Computer-aided design ICCAD '05**

Publisher: IEEE Computer Society

Full text available: pdf(781.16 KB) Additional Information: full citation, abstract

RF circuits for multi-GHz frequencies have recently migrated to low-cost digital deep-submicron CMOS processes. Unfortunately, this process environment, which is optimized only for digital logic and SRAM memory, is extremely unfriendly for conventional analog and HF designs. We present fundamental techniques recently developed that transform the RF and analog circuit design complexity to digital domain for a wireless RF transceiver, so that it enjoys the benefits of digital approach, such as pro ...

17 User cube: a taxonomy of end users

William W. Cotterman, Kuldeep Kumar

November 1989 **Communications of the ACM**, Volume 32 Issue 11

Publisher: ACM Press

Full text available: pdf(952.69 KB) Additional Information: full citation, abstract, references, citings, index terms, review

The user cube, a precise and comprehensive graphical taxonomy designed to provide a common base for understanding and classifying end users in organizations, can be used to assess the risks associated with end-user computing.

18 A computer communication technique using content-induced transaction overlap

Simon Y. Berkovich, Colleen Roe Wilson
February 1984 **ACM Transactions on Computer Systems (TOCS)**, Volume 2 Issue 1
Publisher: ACM Press
Full text available: pdf(988.70 KB) Additional Information: full citation, references, citings, index terms

Keywords: associative proceeding, communication protocol, data compression, multiaccess channels

19 The reflexive CHAM and the join-calculus

Cédric Fournet, Georges Gonthier
January 1996 **Proceedings of the 23rd ACM SIGPLAN-SIGACT symposium on Principles of programming languages POPL '96**
Publisher: ACM Press
Full text available: pdf(1.54 MB) Additional Information: full citation, references, citings, index terms

20 Route Recovery Mechanisms for Ad Hoc Networks Equipped with Switched Single Beam Antennas

Tarun Joshi, Hrishikesh Gossain, Carlos Cordeiro, Dharma P. Agrawal
April 2005 **Proceedings of the 38th annual Symposium on Simulation ANSS '05**
Publisher: IEEE Computer Society
Full text available: pdf(182.99 KB) Additional Information: full citation, abstract, index terms

In this paper we propose a novel three phase route recovery mechanism for routing over switched single beam directional antennas. We enhance the popular Dynamic Source Routing (DSR) protocol to the underlying directional layer and include an improved broadcast mechanism to facilitate an efficient route discovery. In the event of a link failure, our optimized directional routing protocol (DRP) proceeds in three phases to recover the route to the destination: (i) antenna beam handoff, (ii) local r ...

Results 1 - 20 of 91 Result page: **1** 2 3 4 5 next

Google

dpa redundant hardware | Search | Advanced Search | Preferences

Web

Results **1 - 10** of about **53,000** for **dpa redundant hardware**. (**0.15** seconds)

[DOC] resilient to non-invasive attacks, such as **DPA** (Differential Power ...
File Format: Microsoft Word - View as HTML
... a key role in **hardware** design inherently resistant to non-invasive attacks ... of erroneous symbols with moderate **redundancy** of the code (and **hardware**) ...
mark.bu.edu/papers/166.doc - Similar pages

[PDF] Lecture Notes in Computer Science:
File Format: PDF/Adobe Acrobat - View as HTML
the **hardware redundancy** in balanced gate designs, there are many faults which .... (**DPA**) attack was simulated on a substitution box (Sbox) of the Data ...
mark.bu.edu/papers/191.pdf - Similar pages

[PDF] Energy-aware design techniques for differential power analysis ...
File Format: PDF/Adobe Acrobat
algorithmic noise (thereby foiling **DPA**) and saving power. (to amortize the cost of **redundant hardware** instantiation). 3. POWER MASKABLE ...
ieeexplore.ieee.org/iel5/8647/27397/01218775.pdf - Similar pages

[DOC] RGU - IT Disposals Policy
File Format: Microsoft Word - View as HTML
The price will be set at a level to cover both the University's and GEC's costs for the disposal of **redundant hardware**. The price will be set at a level ...
www.rgu.ac.uk/files/Draft%20RGU%20IT%20Disposals%20Policy%20v1.doc - Similar pages

ACIS Users Guide -- Overview
ACIS has two **redundant** Back End Processors, responsible for the overall control of the ... Each BEP is powered by one side of the PSMC **DPA** Power Supply. ...
acis.mit.edu/acis/swuserA/swuser_overview.html - 13k - Cached - Similar pages

[PDF] Permanent Power
File Format: PDF/Adobe Acrobat - View as HTML
The miniaturisation and rising performance of **hardware** ... **DPA** (**redundant** protection without "single point of failure"). The UPS modules are transformerless ...
www.rittal.fi/services_support/pdf-tiedostot/Esitteet/Perma_power_lr_gb.pdf - Similar pages

[DOC] EAST LANCASHIRE HOSPITALS NHS TRUST
File Format: Microsoft Word - View as HTML
Examples of special responsibility areas include: storage and issuing of spares; disposal of **redundant hardware** and software; service delivery liaison for a ...
www.jobs.nhs.uk/cgi-bin/doc_viewer.cgi?type=hrd&vac_ref=911662316 - Similar pages

Rittal power management: Availability up, costs down. (Power ...
Interruptions to critical business processes, whether due to **hardware** faults, ... (scalability and **redundancy**) and distributed parallel architecture (**DPA**), ...
www.rimatrix5.com/loesung_power.htm - 17k - Cached - Similar pages

Review of CHES 2000, August 17-18, 2000, by Joe Marconis

Three **DPA** countermeasures were presented: key masking with localized operations,

random rotation of key and random insertion of **redundant** symbols. ...
www.ieee-security.org/Cipher/ConfReports/2000/CR2000-CHES2000.html - 20k - Cached - Similar pages

[PDF] Microsoft PowerPoint - FailingGracefully2007.ppt
File Format: PDF/Adobe Acrobat - View as HTML
DPA & countermeasures: >1 billion smartcards made annually have **DPA** ..... Information leakage: SPA / **DPA** / Timing .... extra dedicated/**redundant hardware** ...
www.cryptography.com/resources/whitepapers/FailingGracefully2007.pdf - Similar pages

1 2 3 4 5 6 7 8 9 10 **Next**